Delinea's QuantumLock:

Turning Your High Priority Credentials Into Fortresses Even Quantum Wizards Can’t Crack!

As quantum computing edges closer to mainstream reality, it’s time to rethink how we protect sensitive data. Enter Delinea’s QuantumLock, a cutting-edge feature designed to safeguard your most critical credentials against both present-day threats and the quantum-powered cyber risks of tomorrow.

By encrypting secrets with a human-generated password as the private key, QuantumLock ensures that even if someone gains unauthorized access to your system, they can’t crack the code without the unique QuantumLock credentials.

QuantumLock Explained:

QuantumLock provides an additional layer of security by encrypting secrets using asymmetric encryption, where the private key is a human-generated password.This approach ensures that even if unauthorized individuals gain access to the Secret Server, they cannot decrypt the protected secrets without the specific QuantumLock password. By utilizing quantum-safe algorithms, QuantumLock future-proofs data protection against the anticipated capabilities of quantum computers, which could potentially compromise traditional encryption methods.

Delinea's QuantumLock enhances the security of sensitive credentials by leveraging quantum-safe encryption algorithms, such as CRYSTALS-Kyber, recommended by NIST for resisting quantum computing threats. When applied to a secret in Delinea's Secret Server, QuantumLock encrypts the data with asymmetric encryption, requiring a human-generated password as the private key. This ensures that even if unauthorized access occurs, the encrypted secrets remain inaccessible without the QuantumLock password. Designed for high-value, static data, QuantumLock disables certain automated features like Remote Password Changing and heartbeat, making it ideal for safeguarding administrator credentials, root accounts, and other critical assets against both current cyber threats and future quantum-based attacks.

Use Cases:

QuantumLock is particularly beneficial for securing highly sensitive information, such as:

- Global administrator passwords
- Root account credentials
- Bank account details
- Personal Identification Numbers (PINs)
- Social Security numbers

By applying QuantumLock to these types of data, organizations can ensure that only authorized users with the correct QuantumLock password can access the information, thereby maintaining confidentiality and integrity.citeturn0search1

When to Use:

QuantumLock should be employed when protecting secrets that do not require frequent password rotations or heartbeat checks, as enabling QuantumLock disables features like Remote Password Changing (RPC) and heartbeat.It is ideal for static, highly sensitive data that demands robust protection against both current and future threats.Administrators should carefully manage QuantumLock user groups, ensuring that multiple users are assigned to prevent data loss if a single user forgets their password or is deleted.

For more content like and follow me:  **@bertblevins**

Delinea

By integrating QuantumLock into their security strategy, organizations can enhance their defense mechanisms, ensuring that critical data remains secure even as technological advancements, such as quantum computing, evolve.

Purpose of QuantumLock:

QuantumLock is designed to enhance the security of sensitive data by using a combination of asymmetric and symmetric encryption methods. It aims to protect secrets from being compromised, even if the Secret Server itself is breached. The feature is particularly focused on countering the potential threats posed by quantum computing, which could break current encryption methods.

Additional Use Cases:

Additionally, QuantumLock is suitable for securing highly sensitive information, such as:

- Cloud Global admin passwords
- Critical Local Admin Accounts
- High-Sensitivity Customer Data
- Static API Keys and Encryption Keys
- Securing Multi-Cloud Tenant Admins

When to Use:

It’s ideal for safeguarding global administrator accounts, root credentials, API keys, and encryption certificates, especially in industries like finance, healthcare, and government, where compliance and data longevity are critical. QuantumLock is particularly useful for mitigating long-term risks, such as quantum computing threats, and for scenarios where automated features like password rotation are unnecessary. By applying QuantumLock to these sensitive assets, organizations can ensure robust, future-proof protection for their most critical data and systems.

Key Features:

Asymmetric Encryption:

Uses a public/private key pair where the private key is a human-generated password.

Quantum-Safe Algorithms:

Offers the option to use quantum-safe algorithms like CRYSTALS Kyber-1024 to protect the private key.

Independent Security Layer:

Operates independently of regular permissions and Secret Server login access.

For more detailed information, you can refer to the following:

QuantumLock Overview